Remarks

Status of application

Claims 1-47 were examined and stand rejected in view of prior art. The claims have been amended to further clarify Applicant's invention. Reexamination and reconsideration are respectfully requested.

The invention

For a summary of Applicant's invention, please refer to the annotated Summary provided with Applicant's previously-filed Appeal Brief, filed on November 10, 2007.

Prior art rejections

A. Section 102(e): Dugan et al.

Claims 1-47 stand rejected under 35 U.S.C. 102(e) as being anticipated by Dugan et a1. (US 6,804,711, hereinafter " Dugan"). The Examiner's rejection of claim 1 is representative:

> Dugan discloses a method for controlling interprocess communication, the method comprising:
>
> defining rules (col. 12, lines 45-67 and col. 15, lines 57-67) indicating which system services a given application can invoke using interprocess communication to invoke said system services; (col. 14, lines 55-66 and col. 17, lines 24-41)
>
> trapping an attempt by a particular application to invoke a particular system service; (col.13, lines 50-67 and col. 15, lines 16::24) identifying the particular application that is attempting to invoke the particular system service; and (col. 15, line 47-col.19, line 56)
>
> based on identity of the particular application and on the rules indicating which system services a given application can invoke (col. 20, lines 35-62 and col.21, lines 27-32), blocking the attempt when the rules indicate that the particular application cannot invoke the particular system service. (col. 26, line 42-col. 27, line 18)

For the reasons discussed below, Applicant's invention is distinguishable on a variety of grounds.

Dugan appears far less relevant than the Examiner's previously cited art of Andrews (now withdrawn). In particular, Dugan's teaching is directed to a resource management system for an intelligent communications network -- here, the MCI communication (i.e., telephone) network. This has very little to do with Applicant's invention, which is directed to the specific task (performed within the confines of a computer system) of providing security for interprocess communications that may occur between an application running on the computer system and a system service provided by the computer's operating system (e.g., Microsoft Windows). The two are not even analogous, and presumably the Examiner cites Dugan because of a keyword match on "interprocess communication." However, Dugan uses the phrase "interprocess communication" only once in passing, in Dugan's dependent claim 9 (which begs the question of what support Dugan even provides for this in his specification).

"Interprocess communication" or simply IPC is itself a fairly well-known concept encompassing mechanisms where applications or processes share information, and Applicant makes no claim as to having invented that concept. In the Microsoft Windows environment, examples of interprocess communication includes DDE (dynamic data exchange), OLE (object linking and embedding), and clipboard exchange. In the UNIX environment, "named pipes" is an example. What Applicant does claim to have invented -- and which is absent from Dugan -- is a security system and methodology for controlling IPC-based communications that may occur between processes that operate within the confines of a computer system, including those processes that may operate autonomously (i.e., without user initiation or control).

By way of brief review (from Applicant's specification), IPC is the means by which one process may access another process for the purpose of sending it a message. IPC occurs directly between processes (e.g., between two applications, or between an application and a service) typically without any involvement of the user, or even knowledge that IPC is occurring between two processes. Importantly, the specific vulnerability addressed by Applicant's invention involves the fact that a malicious process (malware) may have been placed on the user's machine, which may compromise

security of the computer. In this scenario, the malware may use IPC to trick the computer's operating system (OS) into granting the malware indirect access to the Internet (or other protected resources), via invocation of OS services that are essentially duped into accessing the Internet on behalf of the malware.

Consider the following example from Applicant's specification.

> [0014] Notwithstanding the fact that a given computer system may be protected by a firewall or an end point security product, these services pose an additional security risk. Stated more generally, interprocess communication provides additional opportunities for breaching security measures employed to protect computer systems. For example, a rogue application can circumvent conventional security measures by using services or interprocess communication to cause another application to perform actions on its behalf. The rogue application uses services or interprocess communication as a proxy to obtain, in effect, an elevation of its security privileges. This elevation of its security privileges enables it to breach security by causing another application or service to perform actions that the rogue application is not able to do itself (according to operating system privilege settings). In addition, the rogue application is able to disguise the fact that it is accessing the Internet by going through another application or service (e.g., an operating system service) in a manner that is not detected by a conventional firewall.
>
> [0015] For example, Windows XP includes a DNS (domain name system) service that performs DNS lookup on behalf of other applications. DNS is itself normally a harmless protocol that contacts a DNS server for translating domain names (e.g., cnn.com) into IP addresses. However, a malicious application has the ability to use Windows' built-in DNS service to communicate with a malicious DNS server. For example, the malicious application may use the DNS service for a DNS lookup of "MySecret.Hacker.com". The DNS server at the hacker site ("Hacker.com") would then get a query from the local DNS server asking

whether it has an IP address for "MySecret". In fact, what the hacker site DNS server receives is a token (string of "MySecret"). At this point, the malicious application may engage in almost unlimited communication with the malicious DNS server using an awkward, but also very effective, protocol.

This presents a substantial vulnerability to computer systems, one which is not addressed by the prior art and certainly not addressed by Dugan.

Applicant appreciates that the Examiner's job is to give the broadest interpretation to the claims as possible. To address that issue, Applicant has amended the claims in an effort to further clarify Applicant's invention. In particular, all independent claims have been amended to clarify that the claimed approach pertains to security for interprocess communication occurring within the confines of a computer system (e.g., desktop PC); the approach does not pertain to a large communication network having several nodes, such as the (large) MCI communication network described in Dugan. For example, claim 1 has been amended to now recite (shown in amended form):

1. (Currently amended) In a computer system operating under control of an operating system supporting interprocess communication, ~~A~~ a method for controlling interprocess communication occurring between an application executing on the computer system and a service provided by the operating system,

As shown, the amendment makes it explicitly clear that the claimed approach pertains to security for interprocess communication occurring within the confines of a computer system, such as a single desktop or laptop PC. Thus, it is not appropriate to attempt to make Applicant's claims read on large communication networks that have little or nothing to do with processes operating within the confines of a single computer. The relationship between Dugan's approach (which occurs on a large communication network) and Applicant's approach for providing security to IPC (which occurs within the confines of a single computer) appears tenuous at best, particularly in view of the current amendments to the claims.

Turning now to the specific teachings cited by the Examiner, Dugan states that mechanisms are employed for instantiating service instances according to an implemented business strategy (e.g., load balancing). The deficiencies of Dugan as a competent prior art reference against Applicant's invention are evident. For example, for Applicant's first claim limitation in claim 1 (i.e., limitation of "defining rules indicating which system services of the operating system a given application can invoke using interprocess communication to invoke said system services"), the Examiner cites three sections, including the following from Dugan (at col. 12, lines 45-67):

> As described in above-referenced co-pending U.S. patent application Ser. No. 09/421,590, the Service Administration component 500 further performs the function of configuring and provisioning the IDNA/NGIN service nodes 204 in accordance with configuration information that SA receives. Particularly, based on the received configuration information, the SA component 500 determines the capabilities of each component at each service node 204, which services and data to distribute to which nodes, which services will run on which server(s) resident at the service node, and which data will be cached to local memory resident associated with IDNA/NGIN node server(s). Particularly, SA deploys configuration rules contained in service profile (configuration) files 580 to a Local (node) Resource Manager ("LRM") component 575 of the NOS system 700 for storage in a local LRM cache located at each service node. As will be described in greater detail herein, these configuration files 580 determine which services to execute at an IDNA node. The LRM first reads this service profile file 580 stored in the local cache at that node, and determines a specific Service Layer Execution Environment ("SLEE"), e.g., a virtual machine, to run a service on in accordance with the rules in the service profile file and, which services are to run actively (as persistent objects) in the SLEE, or are to be instantiated only on-demand.

At best, Dugan is describing here general configuration rules for determining "the capabilities of each component at each service node 204, which services and data to distribute to which nodes, which services will run on which server(s) resident at the service node, and which data will be cached to local memory resident associated with IDNA/NGIN node server(s)." There is no mention at all of anything remotely related to interprocess communication of an operating system, nor is there any discussion as to how an application or client of a service would be restricted or blocked (e.g., because the application or client is untrusted or malicious). Applicant's claim limitation (especially in

view of current amendments) is not so broad as to read on any rule pertaining to any service in any system. Instead, Applicant's claim limitation pertains to the very specific notion of defining a policy specifying whether one process may use interprocess communication of the operating system that the computer or runs under to communicate with the system's services, such as DNS service.

Similarly, regarding Applicant's "trapping" or "intercepting" limitation (i.e., second claim limitation) that specifies trapping of communication between an application and an operating system service, the Examiner points to Dugan's "intercepting signaling at the network periphery," which Dugan states is a simple optimization done for reducing latency and improving robustness by shortening the signaling path; it has no relation to Dugan's "rules" (which the Examiner contends teaches Applicant's first claim limitation). In the field of computer science, many scenarios arise where something needs to be trapped or intercepted, and Applicant certainly makes no claim to have invented the notion by itself. Here in the section of Dugan cited by the Examiner, it is evident that the Examiner is simply lifting bits and pieces of text (e.g., "rules", "intercepting", etc.) from a lengthy description of a large communication network, without regard to whether their context is really relevant to Applicant's claims. To be sure, Applicant's invention is described in terms of a security system for a computer that prevents malware from gaining indirect access to the Internet and thus will, of necessity, employ terminology required to describe such systems. However, it is not sufficient that the Examiner simply find disjointed word matches between Applicant's claims and documents in the prior art. Instead, the context in which the words appear must be given consideration, because patent claim limitations are not a disjointed collection of words but instead words appearing in a specific order and context to define a particular scope.

As was the case with the Examiner's previously-cited art, Dugan has no notion that a particular application (e.g., malware) itself may be unauthorized, and therefore may need its access to sensitive system services controlled. Not surprisingly, a text search of the Dugan patent reveals **absolutely no discussion whatsoever** of "malware", "viruses", "Trojan horses", "worms", or the like. Dugan's specification fails to even mention "interprocess communication," save a passing reference to it in one of the dependent claims. Simply put, Dugan fails to provide sufficient teaching or suggestion to anticipate

Applicant's claimed invention.

All told, Applicant's claims set forth a patentable advance in the area of controlling access of potentially "bad" applications or processes that may compromise computer security, especially through indirect means. Applicant's claims were previously amended to highlight the specific features of Applicant's invention that address the vulnerability posed by interprocess communication, that one application or process may attempt to use interprocess communication to thwart security measures. In this present Amendment, Applicant's claims had been further amended to specify that the claimed approach pertains to security for interprocess communication occurring within the confines of a computer system (e.g., desktop or laptop computer). The claims do not pertain to all possible networks or systems, such as the (large) MCI communication network described in Dugan. In view of the foregoing remarks (and in light of clarifying amendments made to the claims), it is respectfully submitted that the claims distinguish over Dugan and any rejection under Section 102 is overcome.

Any dependent claims not explicitly discussed are believed to be allowable by virtue of dependency from Applicant's independent claims, as discussed in detail above.

Conclusion

In view of the foregoing remarks and the amendment to the claims, it is believed that all claims are now in condition for allowance. Hence, it is respectfully requested that the application be passed to issue at an early date.

If for any reason the Examiner feels that a telephone conference would in any way expedite prosecution of the subject application, the Examiner is invited to telephone the undersigned at 408 884 1507.

Respectfully submitted,

Date: April 23, 2008

/John A. Smart/

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
815 572 8299 FAX